~~SECRET~~

ICS Registry 25X1

SENIOR INTERAGENCY GROUP (INTELLIGENCE)
INTERAGENCY GROUP/COUNTERMEASURES (POLICY)
WASHINGTON, D.C. 20505

ISC

CMte 19-SR

DCI/ICS 0870-87
9 June 1987

MEMORANDUM FOR: Chairman, Information Security Committee
Chairman, Personnel Security Committee
Chairman, Physical Security Committee
Chairman, National OPSEC Advisory Committee

LOGGED
10 JUL 1987
IC STAFF/CSIS

FROM: [redacted] 25X1
Chairman

SUBJECT: Coordination Meeting, 19 June 1987, 1000-1200,
Room 6N02 [redacted] 25X1

REFERENCE: IG/CM(P) Responses to Presidentially Directed Tasks

1. Attachment 1 is a copy of the IG/CM(P)'s first status report on the tasks directed by the President in his Report to the Congress on the Nation's Counterintelligence and Security Countermeasures, Plans, Programs, and Capabilities. During preparation of the report on the assigned tasks, several IG/CM(P) tasks were identified as having not yet received requisite attention. Attachment 2 details those tasks that are assigned to the IG/CM(P) and on which no action was reported in the 15 April initial report. Attachment 2 consists of two parts. One lists tasks that have been assigned to a committee for implementation but were not yet reported as started. The other part lists tasks assigned to the IG/CM(P) that have not yet been assigned to an implementing working group, committee, or person.

2. I would, accordingly, like to meet with all chairmen of the IG/CM(P) committees in executive session to review the status of assigned tasks not yet started. Please be prepared to discuss those tasks assigned to, but not yet begun by, your committee and to recommend a locus for each of the unassigned tasks. I intend to have each of the IG/CM(P) tasks underway prior to the second report to the Chairman, SIG-I, or to have a specific explanation of why a given task could not be initiated.

Regraded Unclassified when separated
from classified attachments

[redacted] 25X1

~~SECRET~~

25X1

SUBJECT: Coordination Meeting, 19 June 1987, 1000-1200, Room 6N02 25X1
25X1

3. I am also concerned that, while the first IG/CM(P) report was noteworthy for the number of tasks initiated, only one task was listed as completed. I recognize that many of the IG/CM(P) tasks are open ended, e.g., security awareness and education. Nevertheless, I encourage your pushing for closure on those tasks that have a discernable end point, and I will ask each of you to discuss your plans to this end no later than the July IG/CM(P) meeting.

4. Please confirm your attendance with by COB 25X1
17 June 1987.

25X1

Attachments:
a/s

25X1

SECRET [redacted]

25X1

ATTACHMENT 1

SENIOR INTERAGENCY GROUP (INTELLIGENCE)
INTERAGENCY GROUP/COUNTERMEASURES (POLICY)
WASHINGTON, D.C. 20505

7 April 1987

MEMORANDUM FOR: ACTING CHAIRMAN, SENIOR INTERAGENCY GROUP-INTELLIGENCE

FROM: [redacted] 25X1
Chairman, Interagency Group/Countermeasures(Policy)

SUBJECT: IG/CM(P) Responses to Presidentially-directed Tasks

The committees of the IG/CM(P) have prepared the attached responses to the policy countermeasures tasks culled from both the President's and Senate's reports on counterintelligence and countermeasures. I have read these responses and concur that they are satisfactory and are now ready for your review before forwarding to the President.

[redacted] 25X1

Attachments:
Responses from the Information Security, Personnel Security, and Physical Security Committees

Regraded Unclassified when removed from Classified attachments

SECRET [redacted] 25X1

SENIOR INTERAGENCY GROUP (INTELLIGENCE)
INTERAGENCY GROUP/COUNTERMEASURES (POLICY)
WASHINGTON, D.C. 20505

(ISCOM) 7 April 1987

MEMORANDUM FOR EXECUTIVE SECRETARY, INTERAGENCY GROUP/COUNTERMEASURES (POLICY)

SUBJECT: Information Security Committee (ISCOM) Implementation Status Report Regarding "President's Report"

This report is in addition to that provided on 30 March 1987 regarding the government-wide implementation of the Stilwell Commission's proposals on managing and controlling classified information. It is based on and is keyed to the list of collated actions appended to the IG/CM(P) Chairman's 24 October 1986 memorandum (DCI/ICS-86-0938). Only the actions from the President's report assigned to the ISCOM are addressed.

I.B.4. Establish minimum training standards in information security.

STATUS: No action to date for government employees but this concept has been implemented in the November 1986 edition of the Industrial Security Manual for Safeguarding Classified Information (DoD 5220.22-M). Now, facility security officers must complete minimal security training. (Please note that DoD 5220.22-M is applicable to the cleared contractors of virtually the entire Executive Branch with two major exceptions - the Department of Energy and the Central Intelligence Agency.)

I.C.1.a. Each agency implement NSDD-197.

STATUS: Defense implemented on 26 February 1986 via DoD Directive 5240.6, "Counterintelligence Awareness and Briefing Program."

I.C.1.b. Reinforce provisions of NSDD-197.

STATUS: See above item.

I.C.2.a. Maintain security awareness of the public at large.

STATUS: No specific action to date.

I.C.2.b. Alert public to the importance of approaches by foreign representatives seeking classified information.

STATUS: No action to date.

I.C.4. Monitor and report annually on accomplishments in security awareness in the contractual sector.

STATUS: Security awareness continues to receive emphasis in several ways. Steps are being taken to expand the distribution of the Security Awareness Bulletin of the Department of Defense Security Institute. Also, the Department is continuing its support of security groups such as the American Society for Industrial Security and the National Classification Management Society. Further, a high-level DoD official recently made a security classification

system presentation at the annual gathering of the American Association for the Advancement of Science.

II.B.1.a. Implement initiatives of the ISOO.

STATUS: The Department of Defense has taken unilateral action in this area as follows:

ISOO # 1 - Minimum security education for original classifiers - implemented in paragraph 1-600 d., DoD 5200.1-R, "Information Security Program Regulation," June 1986.

ISOO # 2 - Agency self-inspections and criteria for internal oversight - not implemented.

ISOO # 3 - Mandatory classification challenge - implemented in subsection 2-103, DoD 5200.1-R, June 1986. (This is essentially similar to Stilwell Commission recommendation 21.)

ISOO # 4 - Presidential statement on overdistribution of classified material - not implemented.

ISOO # 5 - Review automatic and standing distribution lists at least once each year - implemented in paragraphs 7-207 c. and 7-208 b., DoD 5200.1-R, June 1986.

ISOO # 6 - Encourage agencies to place controls on reproduction of all classified information - implemented in subsection 7-305, DoD 5200.1-R. (This is similar to Stilwell Commission recommendation 23.)

ISOO # 7 - Amend Executive Order 12356 to require that classification management have agency head attention and require that management of classified information be included in performance rating systems - Executive Order not changed but security is now part of the performance rating system within the Department of Defense as required by paragraph 9-102 d., DoD 5200.2-R, "Personnel Security Program," January 1987.

ISOO # 8 - White House to ask for OPM review and revision of the security specialist (GS-080) job series - the Deputy Secretary of Defense has requested the same action in response to a recommendation of the Stilwell Commission. (See Stilwell Commission proposal 62.)

ISOO # 9 - President to direct the Secretary of Defense to study feasibility of expansion of Department of Defense Security Institute to train all Executive Branch personnel - not implemented.

ISOO # 10 - President to issue statement about need-to-know - not implemented.

ISOO # 11 - Amend Executive Order 12356 to require additional effective oversight of special access programs - not implemented.

ISOO # 12 - That ISOO coordinate with the Security Committee (SECOM) of the intelligence community the development of educational materials

addressing the damage caused by unauthorized disclosures - not implemented.

ISOO # 13 - President to ask the Attorney General to revise guidelines on the investigation of unauthorized disclosures - not implemented.

Please note that some of the ISOO initiatives are essentially similar to recommendations of the Stilwell Commission that are the subject of the ISCOM's 30 March 1987 report cited above. To this extent, there already is agreement that government-wide implementation should occur, notwithstanding the fact that the National Security Council has not yet approved the ISOO's initiatives.

II.B.2. - Amend ISOO directive to establish minimum degree of accountability for Secret information.

STATUS: No action to date.

II.B.3.a. - Amend Executive Order 12356 regarding special access program oversight.

STATUS: No action to date.

II.B.6. - Require sampling of the correctness of classification in agency oversight programs.

STATUS: No action to date.

II.B.7.a. - Direct a high-level study on transfer of information.

STATUS: No action to date.

II.B.9. - Accelerate negotiation of general security of information agreements; establish more stringent criteria for security reviews; and provide dedicated inspection personnel.

STATUS: Specific action on the first two parts of this was not determined but, with respect to the last part, authorization for additional personnel has been requested and is being considered and evaluated in light of Office of the Secretary of Defense staffing requirements.

II.B.10.a. - Complete implementation of the DoD withholding authority for certain technical data.

STATUS: Full implementation of DoD Directive 5230.25, "Withholding of Unclassified Technical Data From Public Disclosure" is essentially complete in terms of major DoD Component supplemental issuances. However, there remains a lag in putting the new policies into practice.

II.B.10.b. - Establish formal criteria for release of reports.

STATUS: No action to date.

II.B.11.a. - Direct that all agencies have procedures to detect unauthorized disclosures and report such.

STATUS: No action to date.

II.B.11.b. - Direct development of plans for prompt investigation of significant unauthorized disclosures.

STATUS: No action to date.

II.B.11.c. - Use all remedies against violators.

STATUS: This policy has been implemented within the Department of Defense (by subsection 14-102 of DoD 5200.1-R, Information Security Program Regulation); no further action taken to date.

II.B.11.d. - Authorize withholding of payments to contractors to enforce security requirements and revoke clearances for non-compliance.

STATUS: These are essentially the same as Stilwell Commission recommendations 50 and 51; existing policy permits such actions but the National Industrial Security Advisory Committee is to review the situation.

II.B.13. - Enjoin agency heads to comply with Federal Records Disposal Act.

STATUS: No action to date.

II.C.3. - Establish procedures for continually assessing individual reliability to include financial vulnerability.

STATUS: No action to date. (Upon reconsideration, this proposal probably should be assigned to the Personnel Security Committee.)

III.A. - Urge retention in H.R. 4759 of a provision making violation of the Intelligence Identities Protection Act of 1982 a federal crime.

STATUS: Not determined.

III.B. - Develop recommended statutory authority to improve cryptographic security.

STATUS: Not determined.

III.F. - Protection of technical data with space application.

STATUS: The Department of Defense has attempted to support this concept in the past and will continue to do so. (It is suggested that the full text of this recommendation was classified in error; some effort should be made to declassify it.)

III.G. - Welcome the opportunity for joint discussions between Congress and the Executive Branch regarding legislation on unauthorized disclosures.

STATUS: No specific action to date.

As noted at the outset, this report is in addition to the one provided on the Stilwell Commission's proposals. Government-wide implementation of those

proposals should have an immediate and beneficial impact on security and thus they were addressed first.

This status report will be refined and updated during subsequent meetings of the Committee. It has been coordinated with all but three of the Committee's members who were not available.

STAT

Maynard C. Anderson
Chairman

Copy furnished:
DUSD(P)

SENIOR INTERAGENCY GROUP (INTELLIGENCE)
INTERAGENCY GROUP/COUNTERMEASURES (POLICY)
WASHINGTON, D.C. 20505

(ISCOM) 30 March 1987

MEMORANDUM FOR EXECUTIVE SECRETARY, INTERAGENCY GROUP/COUNTERMEASURES (POLICY)

SUBJECT: Information Security Committee (ISCOM) Recommendations Regarding the Government-Wide Implementation of Stilwell Commission Proposals on Managing and Controlling Classified Information

During the third meeting of the ISCOM, which was held [redacted] STAT on 3 February 1986, substantial agreement was [redacted] STAT reached with respect to the possibility of implementing on a government-wide basis many of the Stilwell Commission's proposals on managing and controlling classified information. Subsequently, through the coordination process of this report, other Stilwell Commission proposals in this area have been endorsed by the ISCOM members. Particular dissents are noted.

In determining which of the Stilwell Commission's many recommendations were related to "managing and controlling classified information," the words of recommendation # 64 of Senate Report 99-522 of the Select Committee on Intelligence, the ISCOM Secretariat listed those that had been implemented in the June 1986 edition of DoD 5200.1-R, "Information Security Program Regulation." During the course of the 3 February meeting, one additional Stilwell Commission recommendation was added. Also, with this one exception, it was determined during this meeting that it would be appropriate for government-wide implementation of the Stilwell proposals to take place through amendment of the Information Security Oversight Office's (ISOO) directives. However, precise language for this purpose should be developed and coordinated by the ISOO Director.

The attachment contains the ISCOM recommendations with respect to the Stilwell Commissions's relevant proposals. It should be noted that the ISCOM defers to the Personnel Security Committee (PSC) with respect to item 12 of the attachment.

The ISCOM trusts that this report will be satisfactory and stands ready to provide any further assistance that may be required.

[redacted] STAT

Chairman

Attachment

Copy furnished:
DUSD(P)
Chairman, PSC ✓

FOR OFFICIAL USE ONLY ATTACHMENT

ISCOM RECOMMENDATIONS FOR GOVERNMENT-WIDE IMPLEMENTATION OF STILWELL COMMISSION PROPOSALS ON MANAGING AND CONTROLLING CLASSIFIED INFORMATION

1. Stilwell Commission recommendation # 21 (require challenges to classification) - approved. (The CIA objected on the basis of potential workload.)

2. Stilwell Commission recommendation # 22 (better control for Secret material) - approved.

3. Stilwell Commission recommendation # 23 (better control for reproduction equipment) - approved.

4. Stilwell Commission recommendation # 30 (retention of classified documents) - approved with the caveat that in any reiteration of the recommendation, it must be made clear that disposition of records shall be in accordance with established schedules.

5. Stilwell Commission recommendation # 31 (establishing an annual clean-out day) - approved.

6. Stilwell Commission recommendation # 32 (no working alone with Top Secret or Special Access Program information) - approved. (The State Department and ISOO objected.)

7. Stilwell Commission recommendation # 33 (regarding special access programs) - disapproved.

8. Stilwell Commission recommendation # 44 (checking persons entering or leaving activities and unannounced inspections) - approved.

9. Stilwell Commission recommendation # 45 (reporting repeated security violations) - approved.

10. Stilwell Commission recommendation # 46 (added to the original list - enacting legislation to enhance criminal enforcement in unauthorized disclosure cases) - approved.

11. Stilwell Commission recommendation # 47 (use of all remedies against violators) - approved.

12. Stilwell Commission recommendation # 48 (adjudication of multiple violations) - approved.

13. Stilwell Commission recommendation # 54 (direct reporting channel to the agency head) - approved with the caveat that any government-wide adoption should only encourage heads of agencies to set up direct reporting channels for the senior security official.

14. Stilwell Commission recommendations # 59 (minimum training levels) - approved.

15. Stilwell Commission recommendation # 61 (certification) - approved.

FOR OFFICIAL USE ONLY

31 MAR 1987

Personnel Security Committee
Washington, D.C. 20505

MEMORANDUM FOR: Chairman, Interagency Group/Countermeasures (P)

VIA: Director, Community Counterintelligence and Security Countermeasures Staff

FROM: [redacted] STAT
Chairman, Personnel Security Committee

SUBJECT: Status of Personnel Security Committee Efforts on Implementation of Actions Directed in the President's Report

Listed below are items from the President's Report on which the Personnel Security Committee is taking action. Following each item is a note on current status and planned action. (U)

ENHANCE PROFESSIONALISM OF THE WORK FORCE

1. Expedite review and revision of Security Administration Series (GS-080). (U)

P. 17, President's report. Lead: PSC - OPM

- The Office of Personnel Management expects to have a final draft of the revised GS-080 series ready this spring. (U)

2. Ensure appropriate training for certified security managers and other security specialists in the Security Administration Series GS-080, consistent with the findings of the current OPM occupational study of that series. (U)

P. 18, President's report. Lead PSC - OSD-OPM

° During 1986, DoD devised, tested and implemented a new 080 training course. This three-week course was in its third running in February 1987 and has received favorable comments from DoD components. We will look into the applicability to other agencies of this course or elements of it. The Security Awareness and Education Subcommittee has been tasked with developing additional training recommendations. The Director of OPM plans to examine the entire spectrum of conditions affecting the employment of security professionals to include benefits, quality of life in general, pay incentives, promotional opportunities, etc. (U)

3. Recommend to the NSC practical measures to enhance professionalism of the DoD security work force that are applicable throughout the Federal Service. (U)

P. 17 President's report. Lead: PSC - OSD-OPM

° One such measure was among the Stilwell Commission report recommendations which were reviewed for government-wide applicability in early 1986 by an IG/CM working group chaired by DoJ. This was recommendation #60, which called for uniform training for security officers (page 89 of the report). The working group endorsed the concept of agency-by-agency responsibility for security training to meet individual agency needs; the PSC can help make existing training techniques and curricula more available for agencies to adopt as needed. Recognizing that training alone may be insufficient, an early task of the PSC will be to explore other measures for enhancing security professionalism throughout the Federal Service. (U)

SECURITY EDUCATION AND AWARENESS

4. Accelerate development of education and training programs for DOD civilian and military employees and contractors, and make course materials available to all interested agencies. (U)

P. 18, President's report. Lead: PSC - OSD-SAES

° DoDSI has prepared an ambitious plan for 1987 which, if it can be implemented, will both improve and speed the education and training of contractor employees. CIA is preparing a new briefing program on the hostile threat which emphasizes management involvement. The Security Awareness and Education Subcommittee (SAES) has begun to develop other ideas and to scope existing programs to maximize coordination of effort and assistance to agencies which may wish to enhance their contractor programs. (U)

5. Each agency vigorously implement NSDD-197. (U)

PP. 19 and 27, President's report. Lead: PSC

° NSDD 197 (1 Nov 85) required agencies to provide for reporting of foreign contacts and to create/maintain security awareness and education programs. Most agencies responded to the requirement to report the status of their security awareness programs to the NSC as of 1 Dec 85. The SAES has reviewed the results of this status report and will update it as a first step. Although many agencies were then in basic compliance, some agencies indicated work in progress on various requirements of the NSDD. Subsequent SAES efforts will focus on providing practical assistance to agencies, as requested, in maintaining current and effective programs.

NSDD 197 also required the reporting of contacts with Soviet and Soviet Bloc nationals. Requirements for reporting foreign contacts are included in the new Executive order on standards for access to classified information. (U)

6. Reinforce the provisions of NSDD-197 (1985) to place greater emphasis on security awareness and education programs. (U)

P. 19 and 27, President's report. Lead: PSC

° A two-day planning session will be held in April to develop an agenda for actions to be taken. The SAES will focus on identifying needs for training or services, ways of communicating information and expertise among security educators and ways of sharing products and production resources. Approaches under consideration include development of models or standards for security training, expanded training for trainers, networking among trainers, and improved and more widely available publications and catalogues. See also #2 above.

7. Monitor and report annually on accomplishments in strengthening awareness in the contractual sector. (U)

P. 19, President's report. Lead: PSC

° SAES has been assigned primary responsibility for this task and will discuss approaches during their April planning meeting. Monitoring awareness in the contractual sector is largely a continuous process. DIS and others include education and awareness in their inspections of contractor facilities and contractors in general do a great deal of self-improvement and pooled effort to mutual benefit in this area. (U)

8. Ensure that agencies use all appropriate remedies against employees who violate the law and security regulations. (U)

P. 28 President's report. Lead: ISC

° The new Executive order on standards for access to classified information is expected to address this problem; we will have to wait to see what role, if any, the PSC may have in assisting agencies in this regard. (U)

IMPROVE PERSONNEL SECURITY

9. Expedite the preparation and promulgation of an Executive order, applicable to all people with access, which directs common standards for determining need and eligibility for access, for the process of investigation and reinvestigation at all levels of classification, for adjudication of investigative results, for continuing evaluation of personnel with security clearances, and which provides for effective national-level oversight of these procedures. (U)

P. 27, President's report. Lead: DoJ

° The Executive order is nearing completion. (U)

10. Establish procedures for continuously assessing the reliability--including financial vulnerability--of individuals with access to programs of unusual sensitivity. (U)

P. 27, President's report. Lead: PSC

° DoD has identified among its departments several continuing reliability programs of excellent quality; when properly administered, they appear to be of considerable value. Future tasks of the PSC will include developing guidance for agencies to use in improving existing programs or in implementing them, as needed. (U)

11. Develop procedures for the rapid transmission to agencies concerned of criminal justice information on the public record available to DOJ when Justice is aware that it concerns employees or contractors who may hold security clearances. (U)

P. 27, President's report. Lead: PSC - FBI

° The FBI will develop a recommendation. (U)

12. Require that all cleared employees (including contractors) notify the security office of their respective agencies of all personal foreign travel before departure. (U)

P. 27, President's report. Lead: PSC

- The SAES, with assistance from the Executive Secretary will survey existing regulations and procedures for notification of foreign travel, records keeping, and for guidance and briefings for travelers re the threat, provocations, etc. We intend to develop a model program which agencies can adapt to their needs. (U)

13. Intensify personnel security research to develop more productive and, when possible, less costly investigative techniques and more specific guidelines for determinations of eligibility for access. To the extent that such research leads to major changes in the methodology of judging an individual's bona fides, determine the advisability and feasibility of setting a common investigative scope for Top Secret and SCI access. (U)

P. 27, President's report. Lead: PSC

- A subcommittee has been established under the PSC, consisting of DoD/OSD chairmanship and representatives from CIA and OPM. This subcommittee has begun to scope existing and planned research and will make recommendations regarding both substance and priorities in response to the requirements of the President's Report. (U)

LEGISLATIVE INITIATIVES

- Response for all legislative initiatives: All of the items below are included in the Community's proposed legislative program for the 100th Congress. (U)

14. Urge restoration in Intelligence Authorization Act of clarification of the authority of the CIA, NSA, and DIA to deal with security problems in the areas of drug and alcohol abuse without regard to the provisions of any other law, rule, or regulation. (U)

P. 37, President's report.

15. Strongly support legislation that avoids limiting DOD to a year-to-year numerical ceiling for the conduct of its program. The Secretary of Defense should have the flexibility to employ resources involving polygraph examiners as he sees fit to maximize their contribution to personnel security, albeit with close and continuing Congressional oversight. (U)

P. 39, President's report.

16. Urge legislation that takes determinations concerning access to classified information out of the courts and out of quasi-judicial administrative fora (for example, Merit System Protection Board). (Such legislation would not affect any authority which a court may have to review actions clearly violating established constitutional rights.) (U)

P. 39, President's report.

17. Support the development of a legislative proposal which modifies Title 5 of the US Code to require Government employment applicants to reimburse the government for the cost of investigation should it be determined that entries on the personnel security questionnaire were knowingly falsely made or that material information was purposely withheld. (U)

P. 40, President's report.

STAT

25X1

Next 2 Page(s) In Document Denied

Declassified in Part - Sanitized Copy Approved for Release 2012/03/23 : CIA-RDP89M00699R001000640011-7

ATTACHMENT

GROUP I ISSUES

Assigned to an IG/CM(P) committee, but no status report received as of 8 May 1987:

D. IMPROVE MANAGEMENT

1. Review the Stilwell Commission proposals on managing and controlling classified information for possible government-wide implementation. (U)

P. 337, SSCI report (Item 81). Lead: Information Security Committee (ISC)

6. Change the Federal Acquisition Regulations to designate industrial security for classified contracts as a direct cost. The primary intent of this proposal is to identify and monitor security costs associated with particular contracts. (U)

P. 344, SSCI report (Item 108). Lead: ISC

7. Consideration should be given to greater use of Cost Plus Award Fee contracts as an incentive for fulfilling contract security requirement. (U)

P. 344, SSCI report (Item 109). Lead: ISC

8. Require trained and government-certified security officers in each classified contract, including those for special access programs. (U)

P. 344, SSCI report (Item 110). Lead: ISC

II. SAFEGUARD INFORMATION WHOSE UNAUTHORIZED DISCLOSURE COULD JEOPARDIZE US NATIONAL SECURITY

B. IMPROVING INFORMATION SECURITY

3.b. Modify Executive Order 12356 to require greater controls on special access programs and to give the ISOO Director greater

authority to oversee such programs. The Secretary of Defense should have sole authority to approve defense-related, non-intelligence special access programs. The whole government should conduct a comprehensive review and revalidation of all existing special access programs and associated "carve out" contracts, with an independent assessment by the ISOO Director. Such reviews should be repeated on a periodic basis. (U)

P. 337, SSCI report (Item 82). Lead: ISC

4.a. Expand the ISOO's staff to include a permanent inspection element. ISOO should work with DIS to implement improved training courses on information security and classification management. ISOO and the DCI should also reassess special markings with a view to simplification. ISOO should ensure that agencies designate individuals/positions with responsibility for determining need-to-know access. (U)

P. 337, SSCI report (Item 83). Lead: ISOO/ISC

4.b. Make the formulation of "need-to-know" limitations and procedures an integral part of the development process for new or improved technical collection systems, with plans and costs included in budget proposals for such systems. The Community should also devote increased effort to planning and training for war-fighting situations in which dissemination limits will have to be substantially reduced. (U)

P. 337, SSCI report (Item 84). Lead: ISOO/ISC

5. Other Harper Committee recommendations approved by DoD should be implemented promptly and reviewed for government-wide application. (U)

P. 344, SSCI report (Item 112). Lead: ISC

7.b. Consider simplifying the classification system by establishing two levels, eliminating the current Confidential classification. This streamlining should be preceded by consultation with other countries with whom the United States shares security classification agreements. (U)

P. 336, SSCI report (Item 79). Lead: ISC

8. Ensure implementation of the Stilwell Commission recommendations on National Disclosure Policy not only for military information, but for sensitive intelligence and nuclear matters as well. (C)

P. 344, SSCI report (Item 111). Lead: OSD-State-DoE/ISC

11.e. Promulgate an executive order requiring each agency to establish procedures governing authorized disclosure of classified information to the news media, including background disclosures of information that remains classified. Such procedures should require records for accountability, consultation with originating agencies, and designation of officials authorized to disclose classified information to the media. (U)

P. 336, SSCI report (Item 80). Lead: ISC

12. Consider postponement of new criminal penalties for unauthorized disclosure until after the appeals in the Morison case. The Committee supports continued internal agency and FBI investigations for purposes of administrative discipline as well as prosecution, including use of voluntary polygraph examinations under criminal investigative procedures. DoJ guidelines for leak investigations should be revised to reflect current policy of using administrative sanctions when prosecution is not pursued. (C)

P. 338, SSCI report (Item 85). Lead: DoJ/ISC

C. UPGRADING PERSONNEL SECURITY

1.b. Issue a new Executive Order on personnel security. The order should provide for government-wide minimum standards and procedures and a policy oversight office similar to the Information Security Oversight Office. It should focus exclusively on personnel security programs regarding access to classified information and to sites where classified information is maintained. Drafting of this order should not delay action on other recommendations. (U)

P.334, SSCI report (Item 71). Lead: PSC

2. Establish a national crypto-access program and a similar program for that group of individuals requiring extensive access to major automated information systems processing classified information or any continuing access to specially sensitive systems. (C)

P. 27, President's report. Lead: NSA-CIA/PSC

5.c. Increase personnel security research, including expanded research and evaluation on the wider use of psychological testing in the clearance process, taking full account of individual rights, as well as the implications of recent espionage cases. (U)

PP. 333-334, SSCI report (Item 70). Lead: PSC

5.d. Improve the adjudication process for granting or denying security clearances, with more rigorous standards regarding persons who have committed felony offenses; follow-up measures where persons with admitted problems like drug use are cleared; and a government-wide requirement for training of adjudicators. For the most sensitive positions, a "select in" policy based on demonstrated aptitude for security should be adopted in place of the current "select out" policy based on the absence of proved disqualifying factors. (U)

P. 334, SSCI report (Item 72). Lead: PSC

6.a. Reach agreement on a "single scope" background investigation for all Top Secret and SCI clearances. The uniform policy should provide for: (a) less costly and more timely background investigations and clearances; (b) highest priority for meeting the five-year reinvestigation requirement; and (c) a subject interview in all cases. (U)

P.332, SSCI report (Item 64). Lead: OSD-CIA-NSA/PSC

6.b. Postpone implementation of the proposal for one-time, short duration access by cleared personnel to the next higher level of classified information until Secret clearance requirements and investigations are upgraded and the IG/CM(P) has reviewed the issue. (U)

P. 333, SSCI report (Item 68). Lead: PSC

7. Ensure substantially increased funding for personnel security in all relevant departments and agencies. A government-wide plan should be submitted to Congress to achieve the following goals: (a) elimination of the reinvestigation backlog for Top Secret (including SCI) within four years: and (b) implementation within less than ten years of a program for intensified investigation and reinvestigation for Secret clearances. (U)

P. 332, SSCI report (Item 63). Lead: OSD-CIA-NSA/PSC

8. Establish government-wide standards for the use of contractors to conduct personnel field investigations, including requirements for supervision and quality control, restrictions on use of information, exclusion of contractors from adjudication decisions, and standards for experimentation with new procedures for less sensitive clearances. (U)

P. 332, SSCI report (Item 65). Lead: PSC

9.a. Consider government-wide adoption of the Stilwell Commission recommendations to prohibit the practice of requesting security clearances solely to provide access to a controlled area, where there is no need to know or even to be exposed to classified information. Reliability investigations should still be conducted in such cases, with standards equal to those proposed by this report for Secret clearances. (U)

P. 333, SSCI report (Item 66). Lead: PSC

9.b. Reduce the number of clearances held by industry. The DoD goal of a ten percent reduction in FY 1986 should be applied by the DCI (for SCI programs) and the Secretary of Energy. (U)

P. 344, SSCI report (Item 107). Lead: ISC

10.a. Establish more effective means for investigating and clearing immigrant aliens and foreign nationals overseas who are granted access to classified information. (U)

P. 333, SSCI report (Item 67). Lead: PSC

10.b. Ensure full coordination of departmental policies and practices for the use of polygraphing in personnel security screening, to maintain stringent quality controls and safeguards for individual rights, to prevent over-reliance on this technique, to provide for necessary research and funding, and to improve understanding of the procedures. (U)

P. 335, SSCI report (Item 74). Lead: PSC

11. Initiate a pilot program for assignment of DIS personnel to large sensitive contractor facilities on a full-time basis, and the results should be reviewed as a basis for similar government-wide practice. (U)

P. 343, SSCI report (Item 105). Lead: ISC

D. IMPROVING OPERATIONS SECURITY

2. Conduct an overall review of the alerting systems (for example, SATRAN) that provide warning of overflights by air and space platforms to determine the adequacy and effectiveness of such systems. (S/NF)

P. 25, President's report. Lead: DoD/NOAC

4. Develop government-wide operations security (OPSEC) objectives and ensure that relevant agencies have the necessary resources and programs to achieve those goals. (U)

P. 331, SSCI report (Item 61). Lead: NOAC

GROUP II ISSUES

To be undertaken by an ad hoc working group on the IG/CM(P), but no action undertaken as of 8 May 1987:

I. ENHANCE PROFESSIONALISM OF THE WORK FORCE

B. IMPROVE TRAINING

1. Make the adequacy of security training an item of recurring interest for agency Inspectors General. (U)

   P. 18, President's report. Lead: IG/CM(P)-Work Group (WG)

2. Consider phased assignment of national responsibilities for security training to the Defense Security Institute, with an interagency group including representatives from US counterintelligence agencies to develop security awareness materials and with a West Coast annex. (U)

   P. 331, SSCI report (Item 60). Lead: OSD-IG/CM(P)-WG

3. Establish government-wide security training objectives and require minimum levels of training and certification for industrial security officers, clearance adjudicators, and other positions requiring consistent standards. (U)

   P. 331, SSCI report (Item 59). Lead: IG/CM(P)-WG

C. INCREASE SECURITY AWARENESS

3. Strengthen interagency procedures for bringing possible espionage cases to the FBI's attention in a timely manner. The FBI should also be informed when employees with access to extremely sensitive information, such as Howard and Pelton, resign or are dismissed under circumstances indicating potential motivations for espionage. (C)

   P. 316, SSCI report (Item 13). Lead: IG/CM(P)-WG

D. IMPROVE MANAGEMENT

2. Emphasize commander and manager responsibility for security, including government-wide application of the recent DoD action to incorporate security into performance evaluations and development of more realistic and consistent policies for disciplinary sanctions. (U)

P. 330, SSCI report (Item 57). Lead: OSD-IG/CM(P)-WG

3. Assess requirements for research and analysis on security countermeasures to promote aggressive and balanced efforts government-wide, especially on personnel security. (U)

P. 330, SSCI report (Item 56). Lead: IG/CM(P)-WG

4. Enhance security policy and oversight capabilities in the Office of the Secretary of Defense so as to ensure integration of policies for the various DoD security programs. (U)

P. 329, SSCI report (Item 54). Lead: OSD-IG/CM(P)

9. Evaluate security countermeasures resource priorities for the NSC and OMB on an annual basis. Security resources should be identified by function and program in departmental and agency budget justifications. The administration and the Congress should consider additional ways to implement a more coherent budget process for security programs. (U)

P. 330, SSCI report (Item 55). Lead: IG/CM(P)/Work Group (WG)

II. SAFEGUARD INFORMATION WHOSE UNAUTHORIZED DISCLOSURE COULD JEOPARDIZE US NATIONAL SECURITY

C. UPGRADING PERSONNEL SECURITY

4. Vigorously implement the other Stilwell Commission recommendations on personnel security in DoD with augmented OSD policy oversight, and review them at the NSC level for adoption government-wide. (U)

P. 335, SSCI report (Item 76). Lead: OSD-IG/CM(P)-Work Group